Multimed Tools Appl (2018) 77:26881–26899
https://doi.org/10.1007/s11042-018-5892-x

Securing ubiquitous AR services

Adam Wójtowicz[1] · Rafał Wojciechowski[1] · Dariusz Rumiński[1] · Krzysztof Walczak[1]

Received: 10 May 2017 / Revised: 12 January 2018 / Accepted: 13 March 2018 /
Published online: 27 March 2018

Abstract This article describes a new approach to creating and securing ubiquitous augmented reality (AR) systems. Creation of AR presentations in distributed environments, where AR presentation can be dynamically composed at runtime based on distributed data sources and the usage context, and where new services can be dynamically added by various service providers, raises security concerns related to both service access control and users' privacy. To address this challenge, a generic architecture for deployment of ubiquitous AR services and an application-layer security protocol, which enforces usage of AR content according to semantically described usage policies, are proposed.

Keywords Access control · Security protocol · User privacy · Augmented reality · Semantic web · Mobile applications · Ubiquitous applications

1 Introduction

Augmented reality (AR) technology enables superimposing computer-generated content, such as interactive 2D and 3D multimedia objects, in real time, on a view of real-world objects. Widespread use of AR technology has been enabled in the recent years by remarkable progress in consumer-level hardware performance, in particular, in the computational and graphical performance of mobile devices and quickly growing bandwidth of mobile networks. Augmented reality, with its potential to blend real and virtual objects, creates new opportunities for building immersive and engaging applications. Education [5, 38, 41], entertainment [14, 16, 25], medicine [15, 23, 36], and cultural heritage [10, 19, 37] are examples of application domains in which AR-based systems are increasingly being used.

✉ Adam Wójtowicz
awojtow@kti.ue.poznan.pl

[1] Department of Information Technology, Poznań University of Economics and Business, al. Niepodległości 10, 61-875 Poznań, Poland

Existing AR platforms support mainly two forms of augmentation: *directional augmentation* – based on relative geographical position and orientation of the user's device and fixed coordinates of specific points of interest, and *image-based augmentation* – based on image matching and tracking. The advantage of image-based augmentation results from the fact that synthetic content is directly aligned with a view of real-world objects. However, due to limitations of the available image matching algorithms, image-based AR applications are built independently for specific purposes. A user has to install a new application to be able to access new content. Yet, taking into account the diversity of application domains and information that can be presented using AR technology, the most promising are ubiquitous environments, in which different kinds of augmenting content can be contributed by different users and providers. In such systems, AR presentations can be created dynamically based on the available data sources and the current context, through selection of data and automatic composition of AR scenes.

To enable creation of ubiquitous AR environments, the concept of *Contextual AR Environments* (*CARE*) has been proposed [32, 33]. CARE enables the creation of AR presentations, which combine the advantages of both directional and image-based augmentation. In CARE, AR presentations use image-based augmentation, but they are dynamically composed in real time based on the current context and multiple distributed data sources. Contextual creation of AR presentations enables access to a variety of data sources, guarantees scalability and seamless operation. In CARE, AR presentations are accessed through mobile devices equipped with a camera and are visualized using a dedicated mobile application, called *CARE Browser*, which is capable of presenting rich image-based augmentations coming from various specialized services.

The ability to compose ubiquitous AR environments in real time using content and services that are dynamically added by non-trusted parties [39], triggers synergy between different communities of users and various types of service providers (SPs), but at the same time raises *security concerns* related to the need for access/usage control for AR service/content. Thus, the first goal of this work is to develop a method for building open AR systems that provide SPs with the means of controlling how, when, where, by whom, in which context, generally on what conditions, their AR service/content is allowed to be used, or reused, remixed, recomposed by third parties. Such precise control of AR usage requires gathering detailed information describing end-users, their attributes, usage patterns, etc., that often is sensitive from the perspective of end-user's privacy. Moreover, AR systems are particularly vulnerable to privacy risks because of always-on sensing and large amounts of data being processed. Therefore, the second goal of this work is to incorporate means for maintaining controlled balance between data-hungry security and the privacy of AR users into the proposed design. The main contribution of this work, namely *SA-CARE* (*Security-Aware Contextual AR Environments*), is a security framework containing:

- application-layer security protocol based on an architecture for interdependent AR services;
- design of trusted security middleware;
- semantic representation of access/usage control policies for AR content/services and privacy policies for AR end-users;
- identification and detailed description of the use case scenario for the proposed system.

The protocol assures access control that is fine-grained, since precise semantically described AR usage policies are employed, and – at the same time – access control that is comprehensive, due to taking into account the interests of all stakeholders, namely end-users, scenario providers, trackable object providers, multimedia content providers

and business dataset providers. It allows interoperability of usage policies of AR services, and therefore decentralized deployment of loosely-coupled ubiquitous AR systems. Furthermore, it preserves user anonymity and privacy according to their preferences.

The remainder of this paper is structured as follows. Section 2 presents the current state of the art in approaches to building interoperable AR systems and the challenges related to AR data security. Section 3 introduces the conceptual architecture of the SA-CARE environment, which enables creating secure ubiquitous AR environments, describes proposed architecture and access control protocol, discusses its security properties, and provides information about the implementation. Section 4 describes an example of application of the proposed approach in a smart city environment. Finally, Section 5 concludes the paper.

2 Background

2.1 Context-aware AR systems

In spite of the current success of AR technologies, many practical applications have a specific purpose and are used in a specific domain. Moreover, the lifetime of such AR systems is relatively short. Applications of this kind do not allow for experiencing AR presentations in a continuous and contextual manner, i.e., regardless of where the user is located (indoor or outdoor), what kind of device type is used, and taking into account user preferences and needs. Thus, new data models and approaches are required to go beyond the standard techniques of development of AR applications as we know today, to develop continuous, adaptive, and context-aware AR systems. For instance, Schmalstieg and Reitmayr argued that ubiquitous AR systems require independence of the data model from specific applications, and to deal with it, a semantic model of geo-referenced data can be used [34]. The authors derived a data model that allows a suitable degree of semantic reasoning for mobile AR and described how it can be used in urban navigation. Reynolds et al. discussed future directions for mobile AR applications [29] – in particular – how Linked Data can be used in mobile AR browsers for enhancing the reality with information about local points of interest. The authors argue that semantic web technologies can be used for dynamic selection and integration of data from different sources. Furthermore, the use of a cloud of Linked Open Data, such as GeoNames, LinkedGeoData, and DBpedia, can provide a wide range of contextual information for mobile AR browsers. The authors also state that the browsing experience with Linked Data is similar to what we know when we surf the internet using standard web browsers. Another example of using semantic web technologies in an AR system has been presented in [1]. The authors developed a location-based outdoor application that combines Linked Data with domain-specific cultural heritage content. The mobile application explores and visualizes data provided by a back-end server based on a user's GPS location. Hervás et al. presented a ubiquitous AR information system describing context information with the semantic web and QR codes [11]. The authors developed a general model for transforming the physical location of objects into a virtual representation. In order to adapt synthetic content presented in the user interface, the solution requires collecting data provided by an accelerometer and digital compass. QR codes are used to provide data corresponding to a user's location. Nixon et al. demonstrated the *SmartReality* platform that combines AR and semantic web technologies in the entertainment domain [26]. The goal of this AR system is to use Linked Data to provide information about places and events in the vicinity of the user's location. The system uses metadata to select the most appropriate information.

To date, a number of context-aware AR applications have been developed. For instance, in [18], the *Argon AR browser* has been presented, which permits presenting AR content from multiple sources. Argon has been used in various domains such as cultural heritage and community-based AR applications [35]. A contextual approach for indoor navigation using semantic web AR technology has been presented by Matuszka et al. [20]. Similarly to the solution presented by Hervás et al., QR codes are used for recognizing coordinates of indoor locations that are further processed by a server responsible for providing semantically described location information (passages, corridors, exits, etc.) associated with the QR codes. Additionally, the server computes possible paths between two different locations using SPARQL queries. The QR codes are also used for visualization of 3D arrows indicating the direction to a chosen location. In [21] authors present an architecture of a semantically enriched location-based AR browser. On the basis of the user's geographical location, client application retrieves RDF data from DBpedia. The AR interface visualizes 2D annotations representing selected RDF data.

Also, noteworthy tools to model ubiquitous AR applications have been built using web interfaces. For instance, one of the crucial parts of the *OutdoorAR* framework is a web-based authoring application, in which a user can browse, modify, and manage geo-located scenes' information [17]. With this tool, a user is also able to create a new AR scene by specifying the characteristics of the scene, uploading related media assets, and placing them on a map. Finally, these media data can be retrieved by a mobile application that implements the OutdoorAR framework. Another approach, presented in [31], allows users without programming skills to create interactive AR presentations on mobile devices directly on-site. Last, but not least, the designers can also use commercial web-based applications, such as Layar Creator, Wikitude Studio, and Aurasma Studio, to rapidly prototype contextual AR experiences. On the other side, popular low-level libraries such as ARToolKit, Vuforia, ARKit, and ARCore can be used to build AR applications – however, to incorporate contextual approach within the application, sophisticated programming skills are required.

2.2 AR data security

Data security risks are much higher in ubiquitous AR than in regular systems because of continuous mode in which AR systems operate. Complex AR applications require always-recording feature, which can lead to data aggregation phenomenon [12], related mostly to temporal and spatial accumulation of raw visual data that can be privacy-sensitive. It also raises the risks related to user location disclosure (identity privacy, user's position privacy, user's movement path privacy) in the context of user anonymity, unlinkability of user's actions and the strongest requirement of complete unobservability of user actions.

Mobile AR systems employ new input techniques such as voice or gaze-tracking technologies. Usage of these methods, while running multiple applications simultaneously, produces new data security threats related to inaccurate identification of the application that is in focus and should receive input [30]. This threat is even more significant since multiple AR applications expose their APIs to each other and users can share multimedia content between these applications.

Generally, in order to preserve data security in AR systems, access to users' data can be limited by different techniques – separately or as their combinations: policy-based techniques, e.g., formalized XACML security policies; privacy-preserving querying, e.g., based on database anonymizing techniques; techniques dedicated to mobile solutions, e.g., spatial cloaking, etc. However, constant progress in AR techniques in conjunction with the development of mobile infrastructures poses a challenge for the existing systems. In

particular, content processed by multiple AR services interacting dynamically with each other in a mobile environment and provided by distributed SPs cannot be sufficiently protected by current access/usage control approaches.

The most distinguished standardization effort in the domain of protecting the usage of multimedia content is *MPEG-21 REL* – a rule-based access control language [40]. Unfortunately, the *digital item* representation, which is the base for this model, is not expressive enough to support interactive AR presentations with spatially-sensitive composite content contributed by different SPs. Generic languages developed to allow modelling of attribute-based access control, such as *XACML* [22], despite their usefulness in many multimedia protection scenarios, do not support spatial constraints. XACML has spatial extension called *GeoXACML* [27], however, mainly due to its two-dimensional nature and lack of AR interaction protection, GeoXACML is not sufficient for AR frameworks. The same applies to *GEO-RBAC* [4].

It has to be noted that there exist general-purpose security protocols, such as *SAML 2.0* [6] and *OAuth 2.0* [9], that are designed to control access to distributed data or services. Partially they could be utilized as basic building blocks in the process of designing and implementing a secure framework for distributed AR services (e.g., SAML for authentication or OAuth for authorization). However, alone they do not constitute a holistic approach that is required for domain-specific service protection, taking advantage of semantically represented security policies.

There is also AR-specific research on data security focused on user privacy protection. Due to the novelty of the problem, many works only point to forthcoming research directions, but do not present any solutions. An example is [7], in which OS-level access control to AR objects, such as human face or skeleton, is discussed. Other researchers focus on providing AR-specific location privacy [3], however, they propose anonymization-based approach only.

3 Securing contextual AR environments

3.1 SA-CARE architecture

Contextual AR environments consist of *AR presentations*, which are not static as in typical AR systems, but are dynamically composed based on the usage context, including user's preferences and privileges, location, time, device capabilities, previous actions, etc. Typically, contextual AR environments are ubiquitous. For example, a user can walk around a city and observe relevant augmentations using a mobile device equipped with a camera and a dedicated browser application. A contextual AR system, called CARE, has been presented in [32, 37].

To enable dynamic composition of AR presentations in CARE, four types of semantically described elements are used. The first type of elements is a *trackable object*, which is a visual marker representing the real-world objects that can be augmented. The second type of elements is a *content object* representing 2D and 3D multimedia content to be presented in relation to the markers. The third type of elements is a *dataset* related to business services provided in AR environments. The last one is an *AR scenario* describing the course of presentations, i.e., objects being presented, spatio-temporal relationships between the objects, and their behavior. In general, those four types of elements are independent from each other and may be offered by various SPs in a distributed architecture. Discovery and matching between the particular elements of AR presentations are possible based on semantic web techniques.

Both the real-world objects being tracked and the synthetic content being presented depend on the used AR scenarios. For positioning of synthetic content, the browser captures images from the camera and detects *trackable objects*. Synthetic content is generated based on *content objects* and *datasets*. The content objects are media objects (i.e., 2D, 3D, audio, video), while the business datasets are structured data related to the execution of business processes. The datasets can be visualized in an AR environment, and can also be used to control the flow of presentations.

The dynamism underlying creation of AR presentations in CARE with the use of distributed independent data sources requires comprehensive consideration of security aspects. This includes usage control policies (impacting both users' access to services and services' access to users' data) for trackable objects, content objects, datasets, and scenarios; consistency of presentation data and metadata, as well as privacy of users' actions. Below, we present a security-aware extension of CARE, *SA-CARE*.

The main building blocks of the SA-CARE framework are depicted in Fig. 1. Ubiquitous AR environments are created in the form of *AR Presentations* rendered within the *SA-CARE Browser*, which enables a user to interact with the presented content. All components of AR presentations are provided by respective services: *Trackable AR Services*, *Content AR Services*, *Dataset AR Services*, and *Scenario AR Services*. Available services must be registered in the *Semantic AR Service Catalog*. The catalog – together with security-critical system components, i.e., the *User Assertion Provider*, the *Semantic Policy Decision Point*, the *Domain Knowledgebase* and *Ontologies* – form the *SA-CARE Security Middleware*. The particular components of the architecture are shortly presented below.

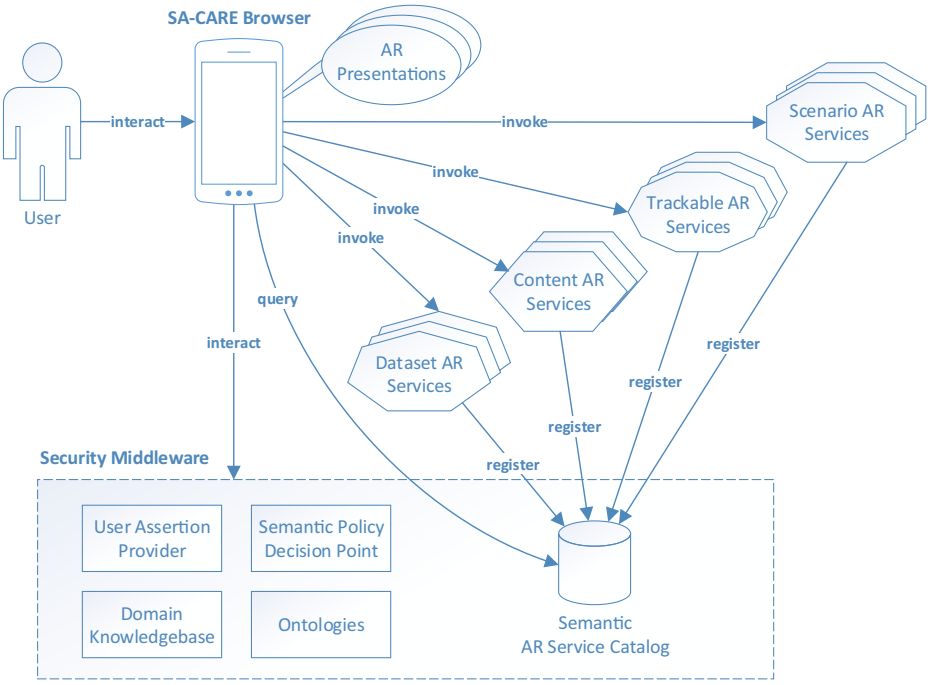

Fig. 1 The main building blocks of SA-CARE

- ***Trackable AR Services*** – provide *trackable objects*, which are binary representations of physical objects. Trackable objects are used for tracking physical objects, which can be augmented with multimedia content. Those services are usually provided by owners of physical objects represented by the trackable objects, e.g., museums may share photos of the cultural objects held in their collections, advertising agencies may publish images of advertising posters.
- ***Content AR Services*** – provide *content objects*, which are used for augmenting physical objects and enabling user interaction. Content objects include 3D models, 2D images, video, audio, and text. Providers of those services can be entities which are either the owners of physical objects being augmented or entities independent of the owners of physical objects providing third-party content.
- ***Dataset AR Services*** – provide *datasets* consisting of texts and numbers retrieved from IT systems of business entities interested in providing services through AR presentations. Business datasets are structured to enable their automatic processing. In general, data retrieved from dataset AR services are not directly visualized within AR environments, but they can be transformed into a multimedia form (e.g., 2D images, 3D models) for visualization. Also, datasets can be used for modifying visual, spatial, temporal and behavioral features of AR presentations. Dataset AR services can be provided by various entities: the owners of physical objects, multimedia content providers or other independent entities such as educational institutions, tourist agencies, municipalities, etc.
- ***Scenario AR Services*** – provide *AR scenarios*, which specify visual, spatial, temporal and behavioral features of AR presentations. Scenario AR services can be offered by different entities, but most often they are business or public entities that are interested in the development of an AR interface to their services.
- ***Semantic AR Service Catalog*** – stores semantic descriptions of both the available services and the data provided through these services. These data are made available in the user's context, which may consist of time, location, user preferences, the status of business services, etc. Given a query sent by the browser, the service catalog responds with the addresses of AR services (trackables, objects, scenarios and datasets) that satisfy the query conditions.
- ***User Assertion Provider*** – provides digitally signed assertions proving authenticity of the values of the user attributes. User Assertion Provider uses internal user database, external data sources or UC Ontology (Usage Control Ontology) to verify claims, if it is required.
- ***Ontologies*** – AR Ontology describes concepts and relations between objects used to model generic AR scenes and interactions. UC Ontology describes security-related concepts and relations. Domain ontologies describe domain-specific concepts and relations that constitute a base for the Domain Knowledgebase. All these ontologies constitute common vocabulary and formalism used for building semantic UC policies for AR scenarios, trackables, content and data objects, for building semantic user privacy policies, and for building Semantic AR Service Catalog. Last but not least, they are used by the Semantic Policy Decision Point in the policy evaluation process.
- ***Domain Knowledgebase*** – in the Domain Knowledgebase, knowledge consistent with the above-mentioned ontologies is stored, describing particular AR services. The Domain Knowledgebase is a data source for the Semantic AR Service Catalog, and for the Semantic Policy Decision Point.
- ***Semantic Policy Decision Point*** – evaluates the UC policies and users' privacy policies taking into account user attributes, ontologies, and the Domain Knowledgebase.

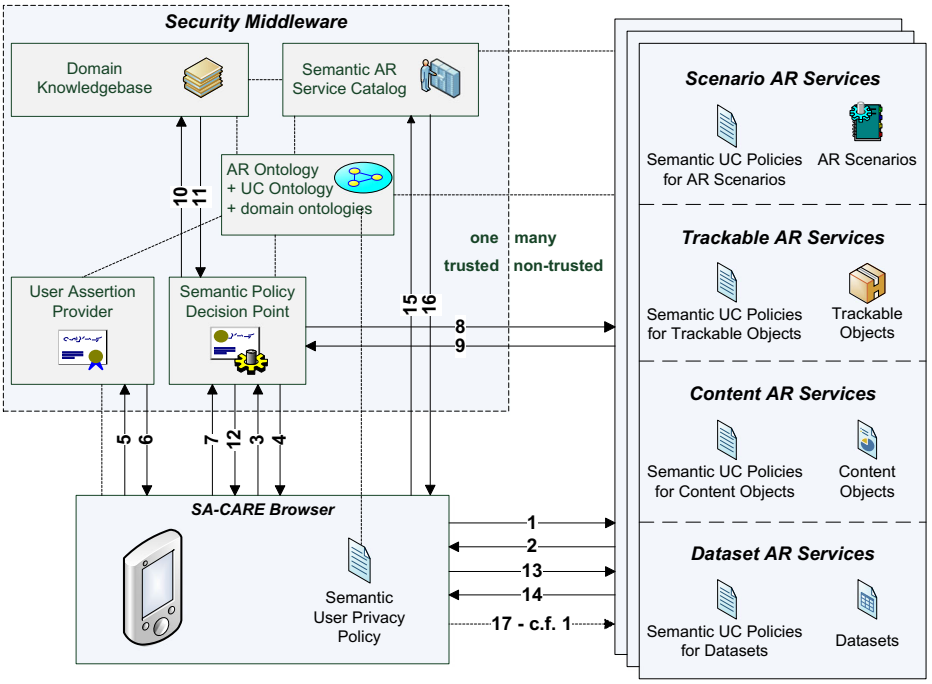

Fig. 2 Steps of the protocol of security-aware semantic usage control for AR

3.2 Access control protocol

To ensure data security and user privacy in ubiquitous contextual AR environments, an attribute-based access control protocol for AR services has been developed. The protocol is used in conjunction with the proposed architecture described in Section 3.1 and depicted in details in Fig. 2. The protocol consists of a number of steps – as presented in the architectural diagram and the data flow diagram in Fig. 3. Execution of protocol steps from the first to the last one (with possible omissions of optional steps) is named protocol course. In practical use cases the protocol is employed multiple times with more than one course (e.g., Section 4.2).

For the clarity of presentation, the diagrams do not show technical messages, which do not influence the logic of the data flow, e.g., digital signature verification steps are intentionally omitted. Also, the procedure of the secure scenario authoring is regulated by a separate protocol, which is out of the scope of this work. As a prerequisite, the *SA-CARE Browser* registers itself at the *User Assertion Provider* and proves its attributes through a secure channel.

The protocol of semantic usage control for AR consists of the following steps:

1. An *SA-CARE Browser* requests an *AR scenario* from a *Scenario AR Service* (this request is denoted as the *initial request*).
2. The *Scenario AR Service* responds with either an *AR scenario* in the case of a publicly available scenario (and then it ends the message interchange process) or a request for a list of selected user attributes that are necessary to evaluate a usage control policy.

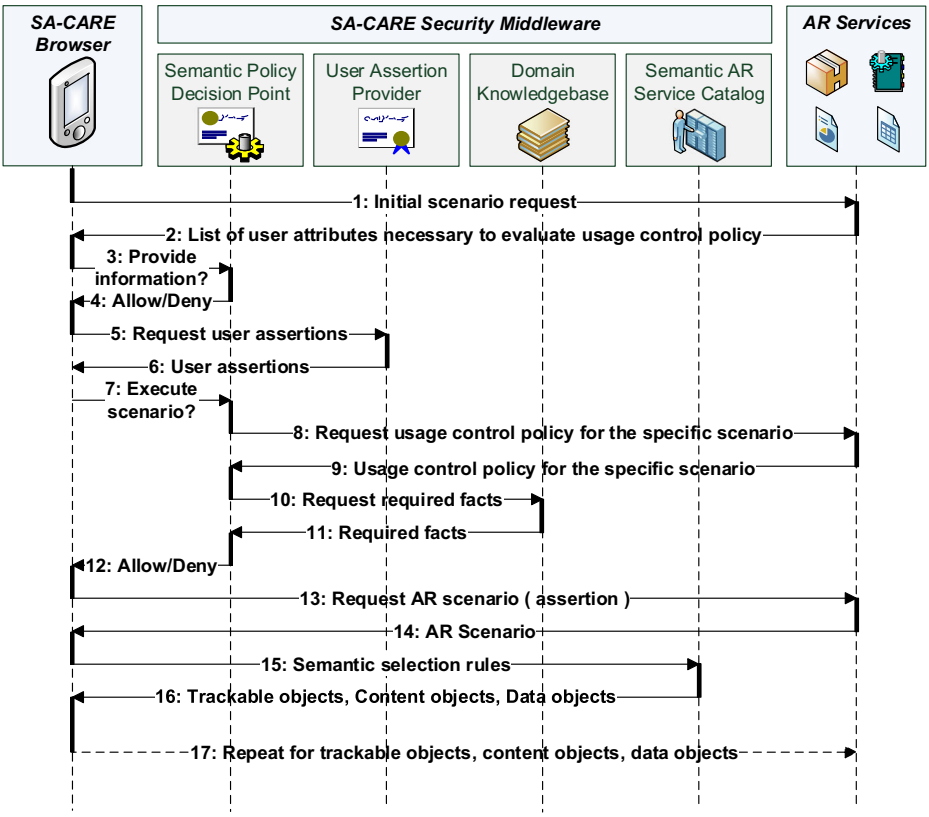

Fig. 3 Data flow in the protocol of security-aware semantic usage control for AR

3. The *SA-CARE Browser* requests the *Semantic Policy Decision Point* for decision whether providing the *Scenario AR Service* with information about itself is allowed according to the *Semantic User Privacy Policy*. The requested attributes and the privacy policy are sent to the *Semantic Policy Decision Point*.
4. The *Semantic Policy Decision Point* evaluates the privacy policy with respect to the initial request.
5. The user, after authentication with a certificate, requests from the *User Assertion Provider* digitally signed user assertions confirming values of the attributes.
6. The *User Assertion Provider* responds with digitally signed user assertions proving authenticity of the values of the requested attributes together with a timestamp.
7. The *SA-CARE Browser* requests the *Semantic Policy Decision Point* for decision regarding the initial request. In the request message, the *SA-CARE Browser* sends also user assertions obtained in the previous step.
8. The *Semantic Policy Decision Point* requests the *Scenario AR Service* for the usage control (UC) policy.
9. The *Semantic Policy Decision Point* receives the UC policy for the scenario from the *Scenario AR Service*.
10. In some cases, knowing the semantic policy and the user attributes is enough for the *Semantic Policy Decision Point* to evaluate the policy with respect to the initial request. However, generally it is required to query the trusted *Domain Knowledgebase*.

11. The trusted *Domain Knowledgebase* sends back the facts required by evaluation process of the policy with respect to the *initial request*.
12. The *Semantic Policy Decision Point* evaluates the UC policy with respect to the *initial request*. The digitally signed result ("allow" or "deny" assertion with a timestamp) is sent back to the *SA-CARE Browser*.
13. Having the "allow" assertion, the *SA-CARE Browser* passes it to the *Scenario AR Service*.
14. In the response message, the *Scenario AR Service* sends the requested AR scenario back to the *SA-CARE Browser*.
15. An AR scenario may contain semantic rules that specify *trackable objects*, *content objects*, *datasets*, and other referenced *AR scenarios*, which are to be used within the scenario at a specific context. Therefore, the *SA-CARE Browser* sends these semantic parameters to the *Semantic AR Service Catalog*.
16. The *Semantic AR Service Catalog* performs reasoning based on semantic data from the *Domain Knowledgebase* and responds with URIs of the required *trackable objects*, *content objects*, and *datasets*.
17. In the subsequent steps, based on the protocol pattern described above (`steps #1-#16`), the *SA-CARE Browser* obtains required data from *Trackable AR Services*, *Content AR Services*, and *Dataset AR Services*.

The most important difference of the data flow in the 2^{nd} course of the protocol concerns usage control to the *trackable objects*, *content objects*, and *datasets* according to their *UC policies*. Before the evaluation of such policy in the `step #7` (in the 2^{nd} or subsequent courses of the protocol), *SA-CARE Browser* sends to the *Semantic Policy Decision Point* not only user assertions, but also scenario "allow" proofs (obtained in the `step #12` of the 1^{st} course). Therefore, the *Semantic Policy Decision Point* "knows" the context of the *trackable objects / content objects / datasets* usage (knows the scenario in which it is going to be used), and *UC policies*, constraining their usage in specified scenarios, can be evaluated.

3.3 Security analysis

Implementations of the proposed framework potentially can be a subject of a number of various attacks on a number of security attributes. However, as the main goal of this work is providing the solution for AR service access control and user privacy protection, attacks in lower layers of the system, implementation-dependent attacks or denial-of-service attacks are out of the scope of this analysis. If confidentiality and authenticity of the messages are secured in the communication channels by means of effective Authenticated Encryption, the passive attacks can be used only to reveal anonymous metadata related to service usage (type of service, when, how long) with standard network/packet analysis. As for active attacks in the application layer, they could be aimed at poisoning the knowledgebase to influence the authorization decisions. This is the main challenge related to the proposed approach: maintaining constant trustworthiness of the knowledgebase (and, to less extent, ontologies) during its lifecycle through automated verification of its consistency with actual implementation of AR services and content. Replay attacks on access control are ineffective due to usage of signed timestamps in `step #6` and `step #12`. Other possible active attack schemes include colluded SPs trying to depict detailed profile of a user by exchanging information about his or her attributes confirmed with collected assertions. This kind of attack can be circumvented by appropriate rules defined in advance by the user in his or her Semantic User Privacy Policy, if the user anticipates the collusion risk. Similarly, attempts

to harvest user assertions with numerous artificial SPs (Sybil attack) can be mitigated with semantically represented rules in privacy policies.

Main advantages of the proposed protocol and architecture for the AR-specific access control are:

1. Fine-grained access control. The authorization decisions are based on the custom and precise attributes (assertions) taking into account AR specificity.
2. Broad range of access control. SPs can limit the usage of their services and content according to specified attributes of end-users as well as specific attributes of other SPs (e.g., trackable object provider vs. scenario provider conflict of interests).
3. Interoperability of the usage control policies. Interoperability is provided due to semantic representations of policy rules, as opposed to low-level technical values or parameters.
4. Applicability for decentralized processing in large-scale and ubiquitous (e.g., city-wide) AR systems:
   - AR scenario providers are independent from trackable object providers, data providers and content object providers. Specialized services can be developed and separation of concerns is maintained.
   - SPs can take advantage of a trusted semantic AR catalog created as an element of the trusted infrastructure.
5. User anonymity and privacy preservation. Due to enforcement of the semantic privacy policy with the provided middleware, end-users can control what data and metadata can be, also indirectly, obtained by SPs – when, by whom, and in what context. Also, the employed attribute-based access control (as opposed to role-based) and user identification based on unlinkable short-term pseudonyms protect the confidentiality of user identities (user privacy).

3.4 Implementation

The SA-CARE approach has been developed on the basis of the service-oriented architecture paradigm. SA-CARE enables semantic modeling of AR environments dividing responsibilities between loosely coupled services distributed on the internet. The services are consumed by software clients running on mobile devices of users, who can move freely in ubiquitous environments. Complex and intensive computation of semantic processing is executed on the server side, while real-time rendering of AR presentations is done on the client side.

The prototype system implemented based on the SA-CARE approach consists of the *SA-CARE Browser* application and a number of RESTful services. The services include: *Semantic AR Service Catalog*, several *Scenario AR Services*, and a number of *Trackable*, *Content*, and *Dataset AR Services*.

- ***Client side.*** The SA-CARE Browser is a client application that runs on a user's mobile device and is responsible for communication with AR services and real-time rendering of AR presentations. The SA-CARE Browser is built on top of the OpenGL ES library [13], which allows to render content objects and data objects provided by diverse vendors. To recognize and track planar images in real time, the SA-CARE Browser uses the *Vuforia* computer vision library [28]. The application collects data from various devices such as: Bluetooth (via the Altbeacon library [24] that provides APIs responsible for getting notifications when beacon devices appear or disappear in the sensing range), GPS (via Android Location Manager to obtain geographical position of end-user), and

also from Android OS and Vuforia to retrieve knowledge about the type of device that is used by an end-user.

The application is based on the REST architectural paradigm and can communicate with multiple distributed AR services. The SA-CARE Browser converts arbitrarily complex Java objects into their JSON representation and vice versa with the use of the GSON library [8] while communicating with AR services. The application has been implemented in *Java* and runs on the *Android* platform.

– ***Server side.*** The architecture of SA-CARE's server is based on Spring and Apache CXF frameworks. The server side is built on top of the Apache Jena SPARQL library. The system consists of a number of RESTful SOA services. The services essential to creating AR presentations are: Scenario AR Services and Semantic AR Service Catalog, which automatically communicate with each other and with the SA-CARE Browser.

The performance of a system built according to the proposed framework strongly depends on the performance of the reasoning in the Semantic Policy Decision Point realized in the `step #12` of the protocol. The reasoning (specifically inference) performance depends on the ontology size and even more on the ontology complexity, as well as on the reasoner itself. For the inference, Apache Jena OWL reasoner is employed. Jena OWL reasoner is slower than the Jena RDFS reasoner about 3-4 times [2]. Thus, if performance issues become critical in a given application, one way of performance improvement is migration to Jena RDFS reasoner on pure RDFS data. The other way is to apply Jena OWL Micro reasoner, which is intended to be close to RDFS performance while also supporting the core OWL constructs. Also, for large-scale deployments, Apache Jena TDB repository should be used for high-performance storage and query.

4 Use case

In this section, an application example demonstrating the practical use of the proposed approach to develop a secure ubiquitous AR environment is described.

4.1 City-wide AR exploration scenario

The use case concerns AR-based exploration of cultural events in a city. The exploration is realized as a two-stage process. In the first stage, a city-wide AR scenario, published by a municipal culture service, is used. The scenario uses trackable objects in the form of common markers visible and recognizable from a far distance, such as bus stop signs, bookshop signs, and other institutions' signs, which are augmented with interactive multimedia content designed to attract user attention (Fig. 4a). When a user activates an interaction element, a second-stage AR scenario is loaded to the SA-CARE Browser.

For example, on a bus-stop shelter several city light boxes are installed. The boxes are maintained by an advertising agency, which uses them for showing advertising posters of their clients. When a user points a smartphone towards a bus stop sign, a new AR scenario, specific to the advertising agency, is started.

One of the city light boxes contains a movie poster downloaded as a trackable object in the second-stage scenario. In the SA-CARE Browser, the poster is augmented with additional data, which allows users to view information and multimedia content related to the movie (e.g., a trailer, a storyline, user reviews, cast), as well as to buy a ticket for a movie

(a) Distant augmentation of the bus stop (screen view).

(b) Close augmentation of the light box (real view).

(c) Close augmentation of the light box (screen view).

Fig. 4 Example of AR scenes in an SA-CARE environment

in a cinema (Fig. 4b, c). The AR presentation is created using trackable objects, content objects, and datasets contributed by different providers:

1. The providers of scenario AR services are the following:
   - municipal information services for the city-wide exploration scenario;
   - an advertising agency or other entity involved in the development of interactive multimedia presentations.
2. The providers of trackable AR services are the following:
   - municipal information services providing first-stage scenario trackable objects;
   - a movie distributor or an advertising agency that can create a trackable object based on a poster image provided by the distributor.
3. The providers of content AR services are the following:
   - a digital art agency (a movie distribution company) providing multimedia data related to the movie (e.g., a trailer, photos);
   - an advertising agency or other entities providing multimedia content required to build a user interface for AR scenarios.
4. The providers of dataset AR services are the following:
   - popular movie websites providing reviews and user opinions on movies;
   - cinemas providing information on tickets for movies and the services for buying tickets online.

The AR presentation (Fig. 4) is composed of four elements: movie trailer, ticket price, buy ticket button, and movie rating. A user can interact with the AR presentation, e.g., he/she can play the movie trailer by tapping on the play button. An electronic ticket to a cinema can be acquired by tapping on the buy ticket button.

4.2 Data flow in the scenario

The protocol described in Section 3.2 is employed multiple times in the presented use case – it is used as a basic building-block for message interchange. This section illustrates how it proceeds in the case of AR-based exploration of cultural events in a city.

Initially, the *SA-CARE Browser* – based on recorded user preferences – requests a generic, city-wide exploration AR scenario from a municipal information service. The requested scenario is public, so it is sent back directly to the client (cf. protocol `step #2` – public case). The scenario requires trackable objects, i.e., images of bus stop signs and content objects, i.e., interaction elements enabling activation of the second-stage scenario. The required trackable objects and content objects are obtained by the browser from municipal trackable services and content object services, based on public policies (simple two-step protocol version).

After collecting the required trackable objects and content objects, the generic scenario is executed by the *SA-CARE Browser*. When the user points his/her smartphone towards a bus stop, an interaction element (a button) is overlaid, enabling activation of the second-stage scenario. If the user clicks on the button, a new AR scenario, specific for bus stop city light boxes, is requested. However, in this example the new scenario requires age proof and non-anonymity proof as a part of the usage control policy (`step #2`). The browser verifies whether disclosing these attributes violates the user's privacy policy (`steps #3-#4`), and, if it does not, obtains assertions proving authenticity of the requested attributes (`steps #5-#6`). Next, the browser requests an authorization decision from the decision point (`step #7`), which – after reasoning based on the user assertions and the usage control policy (`steps #8-#9`) – sends the decision assertion back to the browser (`step #12`). In the presented protocol course, querying the *Domain Knowledgebase* (`steps #10-#11`) can be omitted. Then, the decision is passed to the scenario AR service, which can be offered by an advertising agency maintaining city light boxes located at bus stops (`steps #13-#14`).

The AR scenario requires trackable objects representing posters, and for each poster a number of content objects and datasets, such as trailers, photos, cinema ticket prices, and user reviews – in the case of a movie poster. These objects are not hard-coded in the scenario as URIs of the pre-selected services, but they are selected using semantic rules. These rules are evaluated by the *Semantic AR Service Catalog* (`steps #15-#16`) that either has the required knowledge regarding the services and their providers or uses external knowledge sources from the *Domain Knowledgebase*, e.g., about movies. In the subsequent courses of the protocol, a trackable object of a movie poster is obtained from a service provided by a movie distributor, content objects (trailers, photos) are obtained from services offered by a digital art agency, and datasets (cinema ticket prices and user reviews) are obtained from cinema services and movie critics portals.

In the presented example, a movie distributor, as a part of its semantic usage control policy, restricts the use of its trackable objects within scenarios to advertising agencies which are bound by a legal agreement (this constraint contains no hardcoded service URIs, but is again expressed semantically). Therefore, the knowledgebase querying precedes the policy evaluation (`steps #10-#11` are not omitted in this protocol course). Similarly, a movie critics portal, in its semantic usage control policy, allows the use of its data (user reviews regarding a particular movie) only within scenarios that are directly referenced by scenarios provided by municipal information services (anti data harvesting policy), which is also expressed semantically. Thus, in the case of semantic usage control policy for business datasets, the knowledgebase querying precedes the policy evaluation, in the `steps #10-#11` of its protocol course.

When a user points a smartphone camera towards the movie poster, due to the scenario running on the smartphone, the poster is augmented with trailers, photos, user reviews and ticket prices. Also, the user can tap on the augmenting buttons, in order to buy cinema tickets using appropriate business services.

5 Conclusions

The presented SA-CARE approach enables development of a new class of augmented reality applications in which security constraints are applied in the process of dynamic creation of interactive AR presentations. The approach is based on semantically-modeled access control policies, combined with "privacy-by-design" system architecture and a protocol that separates stakeholders' duties and reduces the attack surface. The implemented and tested prototype system proves the validity of the theoretical model.

Acknowledgements This research work has been supported by the Polish National Science Centre (NCN) Grants No. DEC-2012/07/B/ST6/01523 and DEC-2016/20/T/ST6/00590.

References

1. Aart C, Wielinga B, Hage WR (2010) Knowledge Engineering and Management by the Masses: 17th International Conference, EKAW 2010, Lisbon, Portugal, October 11-15, 2010. Proceedings, chap. Mobile Cultural Heritage Guide: Location-Aware Semantic Search, pp. 257–271. Springer Berlin. https://doi.org/10.1007/978-3-642-16438-5_18
2. Apache Software Foundation (2017) Apache Jena Documentation. https://jena.apache.org/documentation/
3. Aryan A, Singh S (2010) Protecting location privacy in augmented reality using k-anonymization and pseudo-id. In: 2010 international conference on computer and communication technology (ICCCT). IEEE, pp 119–124
4. Bertino E, Catania B, Damiani ML, Perlasca P (2005) Geo-rbac: a spatially aware rbac. In: Proceedings of the tenth ACM symposium on access control models and technologies. ACM, pp 29–37
5. Cai S, Wang X, Chiang FK (2014) A case study of augmented reality simulation system application in a chemistry course. Comput Hum Behav 37:31–40
6. Cantor S, Kemp IJ, Philpott NR, Maler E (2005) Assertions and protocols for the oasis security assertion markup language. OASIS Standard
7. D'Antoni L, Dunn AM, Jana S, Kohno T, Livshits B, Molnar D, Moshchuk A, Ofek E, Roesner F, Saponas TS et al (2013) Operating system support for augmented reality applications. In: HotOS
8. Google Inc. Gson – an open source Java library to serialize and deserialize Java objects to (and from) JSON. https://github.com/google/gson
9. Hardt D (2012) The oauth 2.0 framework. http://tools.ietf.org/html/rfc6749.html
10. Haugstvedt AC, Krogstie J (2012) Mobile augmented reality for cultural heritage: a technology acceptance study. In: 2012 IEEE international symposium on mixed and augmented reality (ISMAR). IEEE, pp 247–255
11. Hervás R, Garcia-Lillo A, Bravo J (2011) Ambient Assisted Living: Third International Workshop, IWAAL 2011, Held at IWANN 2011, Torremolinos-Málaga, Spain, June 8-10, 2011. Proceedings, chap. Mobile Augmented Reality Based on the Semantic Web Applied to Ambient Assisted Living, pp. 17–24. Springer Berlin. https://doi.org/10.1007/978-3-642-21303-8_3
12. Jana S, Narayanan A, Shmatikov V (2013) A scanner darkly: Protecting user privacy from perceptual applications. In: 2013 IEEE symposium on security and privacy, pp 349–363. https://doi.org/10.1109/SP.2013.31
13. Khronos Group The standard for embedded accelerated 3d graphics. https://www.khronos.org/opengles/

14. Koutromanos G, Styliaras G (2015) The buildings speak about our city: a location based augmented reality game. In: 2015 6th international conference on information, intelligence, systems and applications (IISA). IEEE, pp 1–6
15. Kugelmann D, Stratmann L, Nühlen N, Bork F, Hoffmann S, Samarbarksh G, Pferschy A, von der Heide AM, Eimannsberger A, Fallavollita P, Navab N, Waschke J (2017) An augmented reality magic mirror as additive teaching device for gross anatomy. Annals of Anatomy - Anatomischer Anzeiger. https://doi.org/10.1016/j.aanat.2017.09.011
16. LeBlanc AG, Chaput JP (2017) Pokémon go: a game changer for the physical inactivity crisis? Prev Med 101(Supplement C):235–237. https://doi.org/10.1016/j.ypmed.2016.11.012
17. Lee GA, Billinghurst M (2013) A component based framework for mobile outdoor ar applications. In: Proceedings of the 12th ACM SIGGRAPH international conference on virtual-reality continuum and its applications in industry. ACM, pp 207–210
18. MacIntyre B, Hill A, Rouzati H, Gandy M, Davidson B (2011) The argon ar web browser and standards-based ar application environment. In: 2011 10th IEEE international symposium on mixed and augmented reality (ISMAR). IEEE, pp 65–74
19. Madsen JB, Madsen CB (2015) Handheld visual representation of a castle chapel ruin. J Comput Cult Herit 9(1):6:1–6:18. https://doi.org/10.1145/2822899
20. Matuszka T, Gombos G, Kiss A (2013) Virtual Augmented and Mixed Reality. Designing and Developing Augmented and Virtual Environments: 5th International Conference, VAMR 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013, Proceedings, Part I, chap. A New Approach for Indoor Navigation Using Semantic Webtechnologies and Augmented Reality, pp. 202–210. Springer Berlin. https://doi.org/10.1007/978-3-642-39405-8_24
21. Matuszka T, Kámán S, Kiss A (2014) Virtual, Augmented and Mixed Reality. Designing and Developing Virtual and Augmented Environments: 6th International Conference, VAMR 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014, Proceedings, Part I, chap. A Semantically Enriched Augmented Reality Browser, pp 375–384. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-07458-0_35
22. Moses T et al (2005) Extensible access control markup language (xacml) version 2.0. Oasis Standard. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
23. Navab N, Heining SM, Traub J (2010) Camera augmented mobile c-arm (camc): calibration, accuracy study, and clinical applications. IEEE Trans Med Imag 29(7):1412–1423. https://doi.org/10.1109/TMI.2009.2021947
24. Networks R Altbeacon. http://altbeacon.org/
25. Nintendo Co. Ltd. Pokemon go. https://www.pokemon.com/us/pokemon-video-games/pokemon-go/
26. Nixon LJ, Grubert J, Reitmayr G, Scicluna J (2012) Smartreality: integrating the web into augmented reality. In: I-SEMANTICS (posters & demos). Citeseer, pp 48–54
27. (2013) Open Geospatial Consortium: Geoxacml standard
28. PTC Inc. (2012) Vuforia Augmented Reality SDK. https://www.qualcomm.com/products/vuforia
29. Reynolds V, Hausenblas M, Polleres A, Hauswirth M, Hegde V (2010) Exploiting linked open data for mobile augmented reality. In: W3c workshop: augmented reality on the web, vol 1
30. Roesner F, Kohno T, Molnar D (2014) Security and privacy for augmented reality systems. Commun ACM 57(4):88–96. https://doi.org/10.1145/2580723.2580730
31. Rumiński D, Walczak K (2013) Creation of interactive ar content on mobile devices. In: Proceedings of international conference on business information systems. Springer, pp 258–269
32. Rumiński D, Walczak K (2014) Semantic contextual augmented reality environments. In: The 13th IEEE international symposium on mixed and augmented reality (ISMAR 2014). IEEE, pp 401–404. https://doi.org/10.1109/ISMAR.2014.6948506
33. Rumiński D, Walczak K (2017) Semantic model for distributed augmented reality services. In: Proceedings of the 22nd international conference on 3d web technology, web3d '17. ACM, New York, pp 13:1–13:9. https://doi.org/10.1145/3055624.3077121
34. Schmalstieg D, Reitmayr G (2007) The world as a user interface: augmented reality for ubiquitous computing. In: Location based services and telecartography. Springer, pp 369–391
35. Speiginer G, MacIntyre B, Bolter J, Rouzati H, Lambeth A, Levy L, Baird L, Gandy M, Sanders M, Davidson B, Engberg M, Clark R, Mynatt E (2015) Human-computer Interaction: users and Contexts: 17th International Conference, HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015, Proceedings, Part III, chap. The Evolution of the Argon Web Framework Through Its Use Creating Cultural Heritage and Community–Based Augmented Reality Applications, pp 112–124. Springer International Publishing, Cham
36. Stefan P, Habert S, Winkler A, Lazarovici M, Fürmetz J, Eck U, Navab N (2017) A mixed-reality approach to radiation-free training of C-arm based surgery. Springer International Publishing, Cham, pp 540–547. https://doi.org/10.1007/978-3-319-66185-8_61

37. Walczak K, Rumiński D, Flotyński J (2014) Building contextual augmented reality environments with semantics. In: Virtual systems multimedia (VSMM), pp 353–361. https://doi.org/10.1109/VSMM.2014.7136656
38. Walczak K, Wiza W, Wojciechowski R, Wójtowicz A, Rumiński D, Cellary W (2015) Building augmented reality presentations with web 2.0 tools. Springer International Publishing, Cham, pp 595–605. https://doi.org/10.1007/978-3-319-19713-5_52
39. Walczak K, Wojciechowski R, Wójtowicz A (2017) Semantic exploration of distributed ar services. In: De Paolis LT, Bourdot P, Mongelli A (eds) Augmented reality, virtual reality, and computer graphics: 4th international conference, AVR 2017, Ugento, Italy, June 12-15, 2017, Proceedings, Part I. Springer International Publishing, Cham, pp 415–426. https://doi.org/10.1007/978-3-319-60922-5_32
40. Wang X, DeMartini T, Wragg B, Paramasivam M, Barlas C (2005) The mpeg-21 rights expression language and rights data dictionary. IEEE Trans Multimed 7(3):408–417
41. Wojciechowski R, Cellary W (2013) Evaluation of learners' attitude toward learning in aries augmented reality environments. Comput Educ 68:570–585. https://doi.org/10.1016/j.compedu.2013.02.014

Adam Wójtowicz PhD, is an Assistant Professor working at the Department of Information Technology, Poznan University of Economics and Business in Poland. His research interests are focused on information, system and user security, particularly on new access control methods for multimodal and context-aware systems, on security in the Internet of Things and in VR/AR systems, and on privacy preserving systems. He is an author of twenty five publications, many reviews, and he has been involved in a dozen research projects. He lectures on IT System Security, Information Security in Organizations, E-business Security, and Computer Programming.

Rafał Wojciechowski received the M.Sc. degree in Computer Science from the Poznań University of Technology in 2001. Since 2001 he has been with the Department of Information Technology at the Poznan University of Economics. In 2003 he received an EU Marie Curie Fellowship for 9-month training at the University of Sussex (UK). He received the Ph.D. degree in Computer Science (specialization: multimedia systems) in 2008 from the Gdańsk University of Technology. His research interests include Virtual and Augmented Reality, Interactive learning, Service-Oriented Architecture, Business Process Management, Database Systems, E-Government, and Mobile applications.

Dariusz Rumiński MSc, is an Assistant Professor working at the Department of Information technology, Poznań University of Economics and Business. His research interest include Augmented Reality, mobile HCI, Semantic Web, IoT. He is a member of research team (labvr.pl). At the university, he lectures computer programming, software design patterns, designing multimedia applications, and android programming. Currently, he is focused on finalizing his PhD thesis: "Semantic modeling of contextual augmented reality environments", which is expected to be completed in 2018.

Krzysztof Walczak received the M.Sc. degree in Electronics and Telecommunications in 1992 and in Computer Science in 1994, both from the Poznań University of Technology, Poland. He received the Ph.D. degree with distinction in Computer Science in 2001 from the Technical University of Gdańsk. In 2010 he received habilitation degree from the Gdańsk University of Technology. From 1992 to 1996 he was with the Franco-Polish School of New Information and Communication Technologies in Poznań. He spent over one year as an invited researcher at Universities in US and France. In 1996 he joined the Department of Information Technology at the Poznań University of Economics and Business, where currently he is an associate professor and the head of VR/AR research laboratory (http://labvr.pl/).

His current research interests include multimedia systems, human-computer interfaces, virtual and augmented reality systems, and multimedia data repositories. He was acting as a technical coordinator in numerous research and industrial projects in these domains.

He has authored or co-authored 2 books and over 120 research articles published in books, journals and proceedings of international scientific conferences. He is also the author of several European and US patents. He was a member of 130 program committees and 15 organizing committees of international scientific conferences. He is a member of editorial boards of 7 scientific journals. He worked as independent expert for the European Commission and the Polish Ministry of Science and Higher Education. He received numerous awards for his professional achievements.

At the university he lectures advanced internet technologies, future internet, multimedia in business, multimedia technology, and designing multimedia applications.